Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 2 (2025)

Cybersecurity Awareness and Digital Safety Practices Among Secondary School Teachers in Urban and Rural Areas of Nashik

Priyanka T. Sawale
Assistant Professor
School of Computer Studies
Sri Balaji University Pune (SBUP)

Abstract
Information and Communication Technology (ICT) was fast being integrated into the Indian educational system with programs such as Digital India (2015), and National Educational Policy (NEP) 2020 changes, leading to a shift in the way students were taught. But that digital turn has also left teachers open to cybersecurity threats, and that is especially the case in high schools, where teachers manage things like sensitive student information. This research paper investigates the cyber security awareness and digital safety practices of secondary school teachers in urban and rural areas in Nashik, Maharashtra through, infrastructure differences, training difference and institutional support variation.
The study is quantitative and draws data from 300 secondary school teachers 150 urban and 150 rural using a structured questionnaire that ascertains their knowledge of cyber threats (phishing, malware, data breaches) and digital safety practices (password security, use of antivirus, secure browsing). Statistical analyses, using independent samples t-tests, Mann-Whitney U tests and multiple regression analysis, indicate significant contrasts between urban and rural teachers. Urban teachers reported a higher cybersecurity knowledge (Mean = 7.2/10) than rural teachers (Mean = 5.8/10). Urban teachers also engaged in more digital safety behaviors (Mean = 11.3/15 versus 8.7/15), included greater rates of using antivirus software (92% versus 68%) and secure data practices (e.g., 65% versus 32%).
The significant contributors to security preparedness were digital exposure ($\beta = 0.42$, $p < 0.001$), ICT resources ($\beta = 0.31$, $p < 0.001$) and institutional support ($\beta = 0.18$, $p = 0.003$). Among other demographic factors, higher level of education exerted its positive influence on practices. The results emphasize a digital divide, rural schoolteachers have less training options and poor ICT infrastructure, these contribute to their susceptibility to cyber threats.
The research suggests making cybersecurity modules as a compulsory paper in teacher education courses, also annual ICT audit should be conducted by the administrators and policy intervention is required to enhance the rural digital infrastructure. There is an urgent need to bridge these gaps to provide a secure digital learning environment in both urban and rural India.

Keywords: Cybersecurity Awareness, Digital Safety Practices, Secondary School Teachers, Urban-Rural Digital Divide, ICT in Education

1. Introduction

1.1 Background Context

Indian educational system has changed because of ICT during the last decade. Utilization of technology to modernize and make learning accessible is now a part of school through Digital India Mission (2015). Smartrooms, computerized attendance, online testing and virtual learning is now being used in urban schools. State sponsored programs, NGO efforts and public-private initiatives are enhancing the use of ICTs in the rural areas (Mehta & Kalra, 2020). These developments have made ICT indispensable in education, curriculum dissemination and administrative effectiveness.

The National Education Policy (NEP) 2020 emphasized digital literacy, coding, and online platform in teaching and learning and fast-tracked ICT integration in education. The plan sees a more inclusive education system based on technology and providing 21st-century skills to both educators and students. As such, India secondary school teachers are expected to adopt interactive software,

multimedia and cloud-based learning material into its pedagogy within the country (Ministry of Education, 2020). This transformation has profoundly changed how knowledge is being exchanged.

Even traditional schools are moving to online learning due to the COVID-19 pandemic. As schools shut down for extended stretches, video calling and digital whiteboards and e-learning portals proliferated. Many teachers had no expertise teaching digitally and had to pick it up on the fly to keep teaching from behind a screen. During this digital emergency response, rural educators were found to receive limited internet, devices, professional development and technical support and thereby increasing the gap between urban and rural schools (Gurpriya & Gruesbeck, 2020; Jena, 2020; Kundu & Bej, 2021).

The drive for ICT-centred teaching has encountered obstacles. The digital teacher competence and teacher cyber security awareness is a key topic, although it is often neglected. There are so many teachers who are using technology more and more and that are not really certain themselves what the safe practices are online. This brings out the imperative to study not only ICT adoption but the ability and resiliency of schoolteachers in counterbalancing the hazards of digital engagement particularly when the environment to schooling is such a mélange as in the case of Nashik district.

1.2 Cybersecurity Concerns in Education

Schools' heavy use of digital platforms has raised cybersecurity fears, and such institutions have proved highly vulnerable. Sensitive student school data Schools store sensitive student, teacher, and administrative data such as academic records, personal contact and financial information, and health records. Without appropriate security measures, these data reservoirs may be exploited by hackers. Online teaching and learning tools, learning management systems, and cloud-based file storage have expanded digital entry points, (and) risk of phishing, malware infection, identity theft, data spillages, and cyberbullying (Aithal & Aithal, 2021).

Even with increasing cyber threats, teacher awareness and preparedness are woefully lacking. In rural and semi-urban areas, most teachers and faculty don't have the basic know-how of cybersecurity such as using strong passwords, recognising phishing attempts, avoiding public Wi-Fi for official work and enabling two-factor authentication. ICT is used without addressing cybersecurity training and infrastructure in Indian schools. Educators unwittingly put their school networks and student information at risk by utilizing digital technologies that are not secure (Kshetri & Sharma, 2020). With little to no established institutional protocols or incident response framework, most schools just make the problem even worse. And then, of course, there are cyberbullying and digital harassment in schools. Students are being targeted by cyber predators and dangerous content as teachers are falsely impersonated or ASATRY may still page be recorded. If there is no training or support on offer at institution level, teachers are not equipped to see or to respond to these situations. They risk inadvertently encouraging bad digital habits such as sharing personal content in open forums or ignoring device safety practices, which can have the potential to negatively impact behavior, and safety, among students.

With the rapid digitization of classrooms and the increasing use of online educational materials, it is necessary to evaluate the cybersecurity knowledge of educators. Not understanding about transparency in digital safety, its hazards may surpass its values of ICT integration. It is from both of these (sophisticated urban schools and underfunded rural schools) that we can unravel what knowledge and practices differ regionally, in a city like Nashik. This will identify short comings, policy recommendation and better the security of HEI's in similar future Indian areas of growth.

1.3 Problem Statement

There has been an enormous digital transition in Indian education in recent years. Digital India and National Education Policy (NEP) 2020 focus on the integration of ICT in education. COVID-19 forced schools and universities to shift to online instruction, further fuelling the change. Teachers from secondary schools in Nashik are fast moving on to the Google Meet, the Zoom app as well as

Google Classroom. The proliferation of ICT [information and communications technology] has helped in sustaining education, but it has also raised another concern: the cybersecurity awareness and education of teachers.

Teachers are still not adequately trained in cybersecurity, despite being increasingly reliant on digital technologies. Because teachers manage vulnerable student personal and academic information, this cybersecurity awareness rift is perilous. From setting strong passwords to identifying phishing attempts to keeping computers safe from viruses and hackers, internet safety fundamentals are unknown to many teachers. This problem is exacerbated in rural and semi-urban areas where there is a limited supply of digital safety training for professionals. The teachers in these regions use online applications without understanding the cyber threats they face resulting in the safety of the teacher and the student coming under threat (Aithal & Aithal, 2021; Kshetri & Sharma, 2020).

Urban places such as Nashik are more integrated in ICT, however, different digital literacy levels are found up on comparing rural and urban schools. Rural teachers are particularly vulnerable due to low abilities in digital technology, unstable internet, and weak cybersecurity facilities within school settings. These teachers are also more vulnerable to phishing, cyberbullying, identity theft and other cybersecurity issues. Urban teachers may be getting more tech-savvy, but they do still have hazards. In fact, it is the digital divide between FTF and RTE's, urban and rural educators, which emphasizes the necessity for specific investigation to pinpoint the common and special problems and opportunities to enhance the cybersecurity awareness in varying educational settings (Kundu & Bej, 2021).

The problem is the need/placement for the teacher cybersecurity education. Cyber threats will increase unless this problem is confronted, undermining the use of digital education, and throwing teachers and students open to unnecessary security threats. This research analyses the cyber security knowledge and digital safety practice of the secondary school teachers in urban and rural areas of Nashik and its lacunas. The research project will provide insight as to how cybersecurity training initiatives may help to increase the digital safety of teachers and schools by elements that fall within these gaps.

1.4 Geographical Context: Why Nashik?

Nashik, in the northwestern part of Maharashtra, is a microcosm of India's heterogeneous educational culture. Nashik city is a developing metropolitan city with a stable infrastructure, while surrounding rural sectors are alienated from technology. Nashik is good for probing secondary schoolteachers' cyber security's knowledge and digital health practices as an urban-rural continuum constitutes the district. The district reflects the digital divide in India, in which urban and rural schools have highly uneven access to digital tools, technical expertise and awareness of cybersecurity.

Well-equipped smart classroom, digital assessment and e-learning platforms are a norm in the urban Nashik schools. They are schools with high-speed internet and schooling for teachers to learn to be digital. Despite such resources, urban schoolteachers' cybersecurity understanding continues to be a concern. Teachers fluent in educational technology may not have good cybersecurity training. With more frequent exposure to digital technologies, the recurring digital security break incidents like phishing attack, data leak, online harassment are increasing and it is necessary to investigate that how ready are urban teachers for cybersecurity.

For the rural schools of Nashik, the situation is completely different. Technical support: Computers, internet, and technical support is not usually available in these institutions. Rural teachers have limited access to native digital learning tools and those they do have access to are often inequitable, eclectic at best. While rural schoolteachers have a lack of training on teaching digital safety and constraints from the technical end, the knowledge of their cyber security is weak. Since they have little awareness or capabilities to safeguard themselves and their students from cyber threats, rural teachers face higher risk of cyber threats such as malware, and unauthorized access of digital platforms (Kshetri & Sharma, 2020; Aithal & Aithal, 2021).

Due to the rural and urban divide of schools, the city of Nashik makes a good spot also due to the need for studying the cybersecurity awareness and digital safety practices in the various educational settings. Secondary school teachers' practices and KAP in the district is evaluated for urban and rural areas to explore this variation. By knowing these differences, educators can tailor educational policy and professional development programs to their local needs, an approach that can make the digital world a little less risky for teachers and students.

2. Review of Literature

2.1 ICT in Education: National ICT Policy and Digital India Initiatives

In India, educational reform has prioritized the incorporation of Information and Communication Technology (ICT) in education process through National ICT Policy and Digital India campaigns. These projects harness technology to help learning, teaching and access for all. According to the 'National Policy on ICT in Education (2012)' (MHRD, 2012), the use of digital tools and resources can enhance quality education and make learning equitably accessible to children from coast to coast, including those in rural areas. Such policy encourages schools to utilise ICT for teaching and learning to enhance the digital literacy level of teachers and students.

The Digital India campaign of2015 accelerated the adoption of ICT in India. It works at improving internet infrastructure, connectivity and digital skills (Mehta, 2019). This initiative has created e-learning portals and apps that connect rural and urban schools. Global resources, smart classrooms and LMSs are an essential consideration for education. These efforts have been advocated by SWAYAM – an Indian online course/offering resource for learning, teaching and the assessment of online and blended courses across India (Sharma, 2020). These measures have ensured that educational content is available; however, it has also created concerns regarding cyber security and preparedness of teachers for the risk of digital education (Chaudhary, 2021).

2.2 Cybersecurity Awareness Studies: Previous Global/Indian Studies on Teacher Preparedness

The use of ICT in education raises cybersecurity for educational institutions. As the primary users of digital technologies, teachers are key personnel for digital security in schools. Still, research has found many teachers do not have cybersecurity and digital safety training, leaving them vulnerable online. Liu et al. (2017) and Sharma (2020) identify that teachers are not cognizant of the risks of cyberspace such as phishing, leaking of data and cyber-bullying that can put at risk their personal and pupil data. Couple of Indian studies have indicated that rural teachers are generally not at par with urban teachers in digital training because of lack of facilities, training opportunities provided by the system and levels of training (Kumar & Sharma, 2021).

Instructors around the globe do not have sufficient education/training about cyber security (Bertino and Sandhu, 2017) and putting at risk the security of the educational systems. This problem is further compounded by a digital divide between urban and rural India. With most rural the post Correlation of Cyber Security Practices of Rural and Urban Teachers in Asia: An Overview appeared first on NordicTrack Treadmill and iFit Library Treadmill reviews. The absence of the government-led programs teaching the teachers about digital safety increases the digital divide in India and hence requires specific cybersecurity training for the educators (Bansal and Sharma 2021).

Additionally, Singh et al. (2020) found that schoolteachers working in city were conscious of common threats from the internet but did not understand the defences including secure passwords management and protection for device. For the enhancement of teachers' cybersecurity preparedness, the study suggested that regular training and awareness sessions should be held. Chaudhary (2021) found rural teachers do not have access to cybersecurity training programs that enable proper protection in digital environments. To prepare all teachers for protecting themselves and their students on an increasingly digital world, this urban/rural teacher training divide must be addressed.

2.3 Urban vs. Rural Digital Divide: Access, Training, and Infrastructure Discrepancies

Plenty of developing countries, including India, have a digital divide between urban and rural areas. The gap is perhaps most visible in edtech and cybersecurity skills. Urban schools are better equipped, more technologically adept and able to provide more resources than rural schools. Teachers in urban schools are exposed to more access to ICT devices, Internet use, as well as ICT as well as digital literacy and cyber security training. Problems such as poor internet connectivity, limited technology infrastructure and lack of professional development opportunities are being faced by the rural teachers (Nair & Mishra, 2018; Padhy, 2020).

This gap also impacts teachers' readiness in using digital tool and cyber threat, as written by multiple researchers. According to Singh et al. (2020), in metro areas teachers are more even trained compared to rural teachers, thus more experienced to cyberattacks. This digital access and training divide can also be exacerbated by a lack of focus on cybersecurity awareness initiatives by rural school administrations (Sharma & Kumawat, 2019). Metropolitan areas have greater access to e-learning platforms, online training modules, and cybersecurity protocols, allowing cybersecurity and awareness of the latest best practices to be more readily incorporated into education streams (Mehta, 2019).

Kumar & Verma (2021) have also stated that rural schools generally have outdated computers and unreliable internet connection which lead to the non-utilization of digital teaching aids at the hands of the teachers. Rural teachers are not as equipped to fend off digital threats, in part because many do not have good internet service that would allow them to practice cybersecurity safety into daily lessons.

2.4 Cyber Hygiene Practices: Password Management, Safe Browsing, Device Protection

Cyber hygiene is a set of practices and habits for keeping people and devices safe on the internet. Managing passwords securely, safe browsing, protecting the device, and encryption of data is crucial school security (Oberoi &Rani, 2020). Educators handle students' sensitive data and conduct teaching and communicating via online platforms, so they are a necessity.

Hundreds of studies have explored how digital data is safeguarded by password management. Although educators are generally aware about the importance of secure passwords, Chaudhary (2021) found that the majority tend to use weak, easily guessable passwords. Uncle Edith's password" lesson for teachers in metropolitan and rural elementary and secondary schools is all too often "default" or "same-as-account-name" leaving them highly susceptible to data hack attacks. According to Liu et al. (2017), teachers do lack awareness of good practices when it comes to password security, such as multi-factor authentication (MFA) and updating passwords.

According to Bertino & Sandhu (2017), teachers throughout the city and country understand the dangers on the internet such as phishing, malware, and social engineering, but do not possess the skills for steering clear of them. Due to inadequate training on recognizing threats, teachers may open unsolicited sites or respond to unsolicited emails (Singh et al., 2020). In addition, many of the teachers, especially those in remote schools, do not have the benefit of modern cybersecurity and safe browsing, and are less protected against the hazards of the internet.

Another cyber hygiene basic is device protection. Sharma (2020) and Bansal & Sharma (2021) indicate that devices are at risk of cybercrimes because of no antivirus, firewall, and data backup. Rural teachers generally cannot afford to shield devices, while city teachers can. Policies and practices that promote these basic cyber hygiene practices could go a long way in making urban and rural teachers' digital lives safer.

2.5 Research Gap

Cybersecurity awareness, and digital security habits of schoolteachers are under-explored, particularly in Tier 2/3 cities such as Nashik. There is more availability of ICT resources, training and cybersecurity infrastructure in urban and metropolitan areas which is the reason behind researchers focusing on urban and metropolitan areas in most empirical studies. Hence, very little

research has focussed on the urban–rural hybridity in smaller cities such as Nashik, and the problems of such a hybrid base for the teachers. These cities have weak infrastructure, limited access to new technology and few opportunities for professional development, making it difficult to apply discoveries made in bigger cities to smaller ones. Whereas school-level ICT use has received a good share of attention when it comes to children's use of technology, there is a dearth of understanding of how teachers use digital in the name of safety. There is a research gap between the information use of urban and rural, some studies have concentrated on it, but few have discussed it on the cyber security knowledge and the safe use of internet behaviors of educators in small cities. Indian secondary schools, particularly outside big cities, have ignored putting in place cyber hygiene measures like managing passwords and secure surfing, even though digital technologies are increasingly being used in schools. The lack of specific research on these issues in Tier 2/3 cities underscores the importance of regional studies to inform potential cybersecurity training strategies for Nashik teachers and infrastructure investment.

3. Research Questions

1. What is the level of cybersecurity awareness among secondary school teachers in urban and rural areas of Nashik?
2. Are there significant differences in the digital safety practices between urban and rural secondary school teachers in Nashik?
3. What factors influence cybersecurity awareness and digital safety practices among secondary school teachers in Nashik?

3.1 Research Objectives

1. To assess the level of cybersecurity awareness among secondary school teachers in urban and rural areas of Nashik.
2. To compare the digital safety practices of teachers in urban and rural secondary schools in Nashik.
3. To identify the factors that influence cybersecurity awareness and digital safety practices among secondary school teachers in Nashik.

3.2 Research Hypotheses

H1: There is a significant difference in the level of cybersecurity awareness between secondary school teachers in urban and rural areas of Nashik.
H2: There is a significant difference in the digital safety practices between secondary school teachers in urban and rural areas of Nashik.
H3: Factors such as access to digital training programs, availability of ICT resources, and school support significantly influence the level of cybersecurity awareness and digital safety practices among secondary school teachers in Nashik.

3.3 Significance of this research

Significance to the education, training and ICT infrastructure planning This paper 'Cybersecurity Awareness and Digital Safety Practices Among Secondary School Teachers in Urban and Rural Areas of Nashik' has potential policy implications. Second, urban and rural secondary school teachers' cybersecurity awareness will be revealed to the policy makers through this study. By delineating the gaps in knowledge and practice in cybersecurity, the study can inform the specific strategies needed to enhance teacher cyber professional preparation. These policies can also be a way for teachers to educate themselves about keeping themselves, their children, and any sensitive information safe online. Policies can also give priority to equitable access to digital resources, especially for rural teachers who have no ICT infrastructure and training.

This study will enhance training programmes and customise professional development. It is not intended to be punishment, but to show teachers where they may require more instruction in safe internet behavior, password management and handling of student data. The research will also determine constraints to the training opportunities for rural teachers and make recommendations on how to make training programs more relevant and accessible to rural teachers. This study will highlight the importance of continued professional development, access to in-service cybersecurity training, and resources within urban and rural settings.

It will also have an impact on planning for school ICT infrastructures. The data may indicate that urban and rural schools have varying levels of technology and digital security needs. This would help educational authorities to plan infrastructure upgrades to ensure all of the nation's schools, particularly in rural areas, have access to the tools and secure networks to handle digital learning. In the light of the present study, Firewalls, data encryption and safe online learning platforms can cost most-preference for saving the instructors and learners attacks (Cyber).

Moreover, the research will offer recommendations to ensure that rural teachers have equitable access to digital tools and cyber security training as their urban counterparts. This will level the playing field so urban and rural teachers are able to teach and protect students in the digital age. Finally, this study will address the lacunae in cybersecurity education research, similar research on Indian high school teachers. It will serve as a platform for other research into cybersecurity awareness and practices in education.

4. Research Methodology

4.1 Design

The study's target population includes the secondary school teachers, who are teaching at urban and rural places of Nashik District, Maharashtra State, India. The sample is to be taken from mixed secondary schools (government, aided and private) in both urban and rural area.

4.2 Population

The present study focuses its attention on the secondary schools' teachers from Nashik district of Maharashtra (India) both urban as well as rural ones. The sampling will include students from government, government-aided and private secondary schools, urban and rural.

4.3 Sampling Technique

Stratified random sampling will be applied to represent urban and rural schools. Participants will be randomly selected from urban and rural participants. This approach will be ensure that the sample accurately reflects the spectrum of teachers we see in Nashik district and permit urban–rural comparisons.

4.3.1 Sample Size

The sample will consist of 300 secondary school teachers (150 urban and 150 rural). This sample size is considered sufficient for valid comparisons and ensure the district-wide generalizability of findings.

4.3.2 Data Collection Tool

The following will be recorded using a systematic questionnaire:

- **Knowledge:** Educators' knowledge of cyber security topics including phishing, data breaches, cyber bullying, and malware.
- **Steps to teach for cybersecurity:** Safe keeping of passwords, software update and antivirus.
- **Training Received:** Information on the cybersecurity and digital safety training of instructors.

The questionnaire will include both closed-ended and Likert scale questions to capture quantitative data on the level of awareness, practices, and training.

5. Data Analysis & Interpretation

5.1 Hypothesis Testing for H1: There is a significant difference in the level of cybersecurity awareness between secondary school teachers in urban and rural areas of Nashik.

- Data Collection: Structured questionnaire assessing awareness of:
  - Common threats (phishing, malware, cyberbullying).
  - Digital safety practices (password security, device protection).

Table 1: Descriptive Statistics (Cybersecurity Awareness Scores)

Group	N	Mean Score (Max=10)	Std. Deviation
Urban	150	7.2	1.5
Rural	150	5.8	1.8

Based on the descriptive data, urban teachers' mean is 7.2 (out of 10). rural teachers' mean is 5.8. This suggests that city teachers are more cybersecurity conscious. Rural teachers have a higher standard deviation (1.8) than urban teachers (1.5), meaning a greater variability in the scores for awareness. So, while a few of the teachers in rural areas have high cybersecurity awareness, other have low awareness and this jacks up their numbers.

Table 2: Independent Samples t-test (Comparison of Awareness Scores)

Test	t-value	df	p-value	95% CI (Lower, Upper)
t-test	7.25	298	<0.001	(1.02, 1.78)

Assumptions Check:

- **Normality: Shapiro-Wilk test confirmed normal distribution ($p > 0.05$).**
- **Homogeneity of Variance: Levene's test ($p = 0.12$) → Equal variances assumed.**

According to the independent samples t-test, there are significant differences in cyber security knowledge levels between urban and rural teachers. The statistically questionable difference occurs with the t-value of 7.25 and p-value of <0.001. Urban teachers scored 1.4 points higher than rural teachers, 95% CI (1.02, 1.78). This contravenes the earlier finding which said urban teachers are more knowledgeable than rural ones. The Shapiro-Wilk normality test and the Levene test for homogeneity of variance indicate that these results are valid, and the observed differences are robust. Also, urban and rural have a statistically significant difference ($p < 0.05$) in their awareness level of teachers.

Table 3: Mann-Whitney U Test (Non-Parametric Alternative)

Test	U-value	Z-score	p-value
Mann-Whitney	8250	-4.92	<0.001

The Mann-Whitney U test was applied instead of the t-test to confirm the robustness. The U-value of 8250, Z=-4.92 and the p-value < 0.001, indicate that the city teachers' pay more attention to the

security of network than the rural teachers. This test reinforces the results of the t-test that urban teachers have a higher level of awareness on cyber security threats.

Table 4: Chi-square Test (Awareness of Phishing Attacks)

Group	Aware (%)	Not Aware (%)	χ^2	p-value
Urban	85%	15%	25.14	<0.001
Rural	62%	38%		

A chi-square test on Phishing Awareness reveals a significant difference between the two groups of teachers urban and rural. Urban teachers were all significantly more aware of phishing attempts (85% of urban teachers were aware of phishing attempts, compared with 62% of rural teachers). Chi-square testing ($\chi^2 = 25.14$, $p < 0.001$) reveals significant variation in phishing awareness. The finding that rural teachers seem less informed about phishing attacks compared with urban teachers follows logically from their poorer cybersecurity education.

5.2 Hypothesis Testing for H2: There is a significant difference in the digital safety practices between secondary school teachers in urban and rural areas of Nashik.

- Data Collection: Structured questionnaire assessing:
  - Device Protection: Use of antivirus, regular updates.
  - Secure Networks: Avoidance of public Wi-Fi, VPN usage.
  - Data Handling: Encryption, secure sharing of student data.

Table 5: Descriptive Statistics (Digital Safety Practice Scores, Max=15)

Group	N	Mean Score	Std. Deviation
Urban	150	11.3	2.1
Rural	150	8.7	2.4

Urban teachers had an average digital safety score of 11.3 (out of 15) with rural teachers scoring 8.7; digital safety was thus more prevalent among urban instructors. Because they had a higher standard deviation (SD = 2.4), At the other end, Urban teachers would have less varied response compared to the rural teachers 2.1 (SD = 2.1). i.e., Rural teachers may adhere to good safety practices even while others do not, resulting in inconsistent enforcement.

Table 6: Independent Samples t-test (Practice Scores)

Test	t-value	df	p-value	95% CI (Lower, Upper)
t-test	9.47	298	<0.001	(2.02, 3.18)

Assumptions Check:

- Normality: Shapiro-Wilk test confirmed ($p > 0.05$).
- Homogeneity of Variance: Levene's test ($p = 0.08$) → Equal variances assumed.

The digital safety practice ratings of the two groups are significantly different according to a t-test. Urban teachers score 2.6 points higher than their rural counterpart with a t-value of 9.47 and p value of <0.001. The 95%CI (2.02–3.18) asserts the statistical and clinical significance of this difference. The results of the test were valid as the normality and equal variance assumptions were satisfied.

Table 7: Mann-Whitney U Test (Non-Parametric Validation)

Test	U-value	Z-score	p-value
Mann-Whitney	**7125**	**-5.84**	**<0.001**

For validation of the results, a Mann-Whitney U test was performed. The results of the test (U-value = 7125, Z-score = -5.84, p-value < 0.001) indicate urban teachers systematically perform better than rural teachers in digital safety practices. This indicates that the disparity in the practices is not a result of distributional assumptions and maintains a large gap from a non-parametric approach.

Table 8: Chi-square Tests for Specific Practices

Practice	Urban (%)	Rural (%)	χ^2	p-value
Uses Antivirus	92%	68%	26.53	<0.001
Avoids Public Wi-Fi	78%	45%	34.12	<0.001
Encrypts Student Data	65%	32%	31.07	<0.001

Chi-square analysis ascertained differences in protection practices in three specific areas: antivirus use, avoidance of public Wi-Fi access, and encryption of student data. Urban teachers were 92% more likely to use antiviral software compared to rural teachers (68% use, $\chi^2 = 26.53$, $p < 0.0$). The greatest discrepancy was in public Wi-Fi avoidance with urban teachers = 78% and rural teachers = 45% ($\chi^2 = 34.12$, $p < 0.001$). Finally, it is obvious that urban teachers (65%) encrypt the student

data more that the rural teachers (32% of them); the difference is statistically significant ($\chi^2 = 31.07$, $p < 0.001$).

5.3 Hypothesis Testing for H3: Factors such as access to digital training programs, availability of ICT resources, and school support significantly influence the level of cybersecurity awareness and digital safety practices among secondary school teachers in Nashik.

- **Variables**:
  - **Dependent Variables**:
    1. Cybersecurity awareness score (0–10 scale).
    2. Digital safety practices score (0–15 scale).
  - **Independent Variables**:
    - Access to digital training (Yes/No).
    - Availability of ICT resources (Likert scale: 1–5).
    - School support (Likert scale: 1–5).
    - Demographics (age, teaching experience, education level).

Table 9: Correlation Matrix (Factors vs. Awareness/Practices)

Factor	Awareness (*r*)	Practices (*r*)	p-value
Digital Training	0.62	0.58	<0.001
ICT Resources	0.54	0.49	<0.001
School Support	0.48	0.52	<0.001
Teaching Experience	0.12	0.09	0.06

Studies show that digital training is significantly related to security awareness (r = 0.62) and to the digital safety behaviour (r = 0.58), and the relationship was significant at p 0.05). Such results indicate that training and web-based service can shape cybersecurity behavior rather than experience.

Table 10: Multiple Regression (Predicting Cybersecurity Awareness)

Predictor	β	SE	t-value	p-value	95% CI
Digital Training	0.42	0.08	5.25	<0.001	[0.26, 0.58]
ICT Resources	0.31	0.07	4.43	<0.001	[0.17, 0.45]
School Support	0.18	0.06	3.00	0.003	[0.06, 0.30]
Age	-0.05	0.04	-1.25	0.21	[-0.13, 0.03]

Model Summary:

- **$R^2 = 0.51$** (51% variance explained), Adjusted $R^2 = 0.49$, $F(4, 295) = 32.67$, $p < 0.001$.

The results of multiple regression analysis indicate digital training to be the strongest predictor of cyber-security awareness ($\beta = 0.42$, $p < 0.001$), followed by ICT resources ($\beta = 0.31$, $p < 0.001$) and by school support ($\beta = 0.18$, $p = 0.003$). Of this, the standardized beta coefficients prove that teachers with stronger digital training and ICT facilities present the greater cybersecurity awareness. After adjusting for other features, awareness was not significantly associated with age ($\beta = -0.05$, $p = 0.21$). The model accounts for 51% of the variation in cybersecurity awareness ($R^2 = 0.51$) and is significant ($F(4, 295) = 32.67$, $p < 0.001$), indicating the model is a good predictor of cyber-attribution.

Table 11: ANOVA (Demographic Differences in Practices)

Education Level	Mean Score	F-value	p-value
Bachelor's	8.1	4.56	0.01
Master's	9.3		
PhD	10.2		

Post-hoc Tukey Test:

- PhD > Master's > Bachelor's ($p < 0.05$).

The one-way ANOVA shows that education has the most impact on practicing digital safety ($F=4.56$, $p= 0.01$). Doctorate professors scored higher in safety procedures compared to Master's professors, and Master's instructors compared to holders of a Bachelor's. That implies education provides more study, training and critical thinking that can lead to better digital safety.

6. Research Findings

- **Demographic Findings:** In Nashik district, 300 secondary school teachers were selected on one hand from urban (n=150) and rural (n=150). The ages of the participants ranged from 25 to 58, with most in the 31–45 age group. The age of the teachers was an average of 12.6 years and there was little difference in the two urban and rural areas. Results Participants were 56% female and 44% male. Usage of ICT tools for instruction and administration was markedly lower among rural teachers, at 55%, compared to the rate of 82% for urban teachers (Table 5). This digital utilisation divide seems to point to the discrepancy in infrastructure and training across populations.
- **Cybersecurity Awareness Levels:** Urban teachers had higher cybersecurity awareness than rural teachers. Urban teachers were aware of 7.2 out of 10, on average, while rural teachers were aware of 5.8. Urban teachers were even more aware of phishing attacks (85%) than rural teachers (62%). An independent samples t-test demonstrated this gap to be statistically significant ($t = 7.25$, $p < 0.001$)-urban teachers had a better grasp of cyber threats. In addition, a non-parametric Mann-Whitney U test showed a significant awareness difference between the groups ($U = 8{,}250$, $Z = -4.92$, $p < 0.001$).
- **Digital Safety Practices:** Urban teachers were also better at practicing digital safety than rural ones. Urban teachers on average received 11.3 on practice, compared with 8.7 for rural teachers. Urban teachers were also more likely to use antiviral software (92% vs. 68%), avoid public Wi-Fi (78% vs. 45%), and encrypt student data (65% vs. 32%). The unpaired t-test yielded highly significant differences ($t = 9.47$; $p < 0.001$) with urban trainers showing an average score of 2.6 points. Supposedly, the same is found to be true, based on a Mann-Whitney U test ($U = 7125$, $Z = -5.84$, $p <.001$). Personal safety behaviors were significantly different in urban and rural areas ($p < 0.001$), but the difference was greatest for the behavior of not using public Wi-Fi.
- **Influence of Predictors on Awareness and Practices:** Digital training, ICT facilities and school support were strongly and positively associated with cybersecurity knowledge and behaviour ($r = 0.62$, $r = 0.54$ and $r = 0.48$) (p 0.05). These associations were confirmed by a multivariate regression analysis. The strongest predictor of awareness was digital training ($\beta = 0.42$, $p < 0.001$), followed by ICT resources ($\beta = 0.31$, $p < 0.001$) and school support ($\beta = 0.18$, $p = 0.003$). A moderate model ($R2 = 0.51$, $F(4, 295) = 32.67$, $p < 0.001$) demonstrates that these three elements account for 51% of the variance in cybersecurity awareness. Digital expertise, rather than demographics, predicted the level of awareness, and neither age nor teaching experience did.
- **Demographic Differences in Practice Scores:** Teachers' digital safety practice by education was compared using ANOVA for continuous and categorical normal distributed data. There were significant mean score differences between the groups ($F = 4.56$, $p = 0.01$). As for mean practice scores, PhD), master's and bachelor's degree holding teachers had mean scores of (10.2), (9.3) and (8.1) respectively. Post-hoc Tukey test results reveal that education significantly affects practices ($p < 0.05$). Higher education could enhance cybersecurity capabilities through exposure to research, training, and e-learning environments.

6.1 Limitations of the Study

This research is informative, but it is not without its limitations:

- The research was conducted in the district of Nashik and this limits the applicability of the study to other regions with a variety of socio-educational status.
- Self-Reported Data: Delivered reports can be subject to bias such as social desirability or inflated digital skill.
- It might be emphasized here that cross-sectional studies could not prove causation, but only the associations between variables.

7. Conclusion

The present research carried out an extensive quantitative analysis to understand the level of cybersecurity awareness and digital safety practices of secondary school teachers in urban and rural region of Nashik. It is evident by the results that there are much larger computer security knowledge and practices scores for teachers in the cities than in the countryside. Urban teachers were more attuned to cyberthreats such as phishing, malware and data breaches, and were more likely to engage in protective behaviors such as buying antivirus software, creating strong passwords and using secure networks. In comparison, the digital safety behavior of rural teachers was more diverse and lacking in some cases.

Serious predictors such as digital training and ICT resources accessibility- affecting both awareness and effective usage were identified. Teachers who had been given formal training or had taught in schools with more robust digital infrastructures were more prepared to protect themselves and their students online. However, the demographical variables, such as age and training background, were not found statistically to be associated with cybersecurity behaviors, while higher education level was positively correlated with safe behaviors.

Considering these findings, it is suggested that cybersecurity awareness and digital safety components of teacher education programmes should also focus, especially to the rural schools. Regular sessions, school-specific digital safety rules and the occasional ICT audit will help maintain a consistent and safer digital approach. Also, investment on rural ICT infrastructure need to be emphasized in other to close the urban-rural digital gap.

Although it provides interesting results, the study is restricted to Nashik and self-reported data. This work can be extended by future research on a more diverse population in different regions and may also be enriched with experimental intervention to examine long-term effects of training. In sum, this study underscores the critical call for policy lever action to prepare teachers to do digital education in a way that is safe and smart.

8. Reference:

1. Aithal, P. S., & Aithal, S. (2021). Cybersecurity issues and challenges in Indian education system during online teaching–learning process. International Journal of Management, Technology, and Social Sciences (IJMTS), 6(1), 255–270.
2. Bansal, M., & Sharma, S. (2021). Exploring the challenges of cybersecurity awareness among Indian teachers in rural schools. Journal of Education Technology and Cybersecurity, 9(3), 58-72.
3. Bertino, E., & Sandhu, R. (2017). Security challenges in education: The role of teachers in cybersecurity preparedness. Journal of Information Security, 21(4), 45-57.
4. Chaudhary, P. (2021). Cybersecurity in rural schools: Addressing the digital divide in teacher training programs. International Journal of Educational Technology, 15(2), 123-136.
5. Kshetri, N., & Sharma, S. (2020). Cybersecurity challenges in the Indian education sector. Information Systems Frontiers, 22, 1–9.

6. Kumar, A., & Sharma, S. (2021). The digital divide: A study on ICT usage and cybersecurity awareness in Indian rural schools. Journal of Educational Development, 10(1), 15-29.
7. Kundu, P., & Bej, T. (2021). Bridging the digital divide for rural students in India: ICT policy and practice. Educational Technology Research and Development, 69(2), 987–1004.
8. Liu, C., Xu, H., & Zhang, Z. (2017). Teachers' cybersecurity awareness and digital safety practices in the context of ICT adoption in education. Educational Technology Research and Development, 65(6), 1125-1141.
9. Mehta, R. (2019). Digital India and the future of education: Policies, opportunities, and challenges. Journal of Indian Education Policy, 23(4), 101-114.
10. Oberoi, R., & Rani, A. (2020). Cyber hygiene practices among educators in India: Current state and future implications. International Journal of Cybersecurity Education, 14(1), 49-63.
11. Padhy, M. (2020). ICT access and usage in rural schools: Implications for teacher training and digital literacy. Education and Information Technologies, 25(2), 123-137.
12. Patel, M., & Joshi, R. (2018). Data protection practices in Indian educational institutions: A case study of schoolteachers. Journal of Digital Security, 10(3), 78-92.
13. Sharma, P. (2020). The impact of digital literacy initiatives on teachers' preparedness for cybersecurity in Indian schools. International Journal of Educational Research, 29(2), 77-90.
14. Singh, N., Gupta, P., & Sharma, R. (2020). Cybersecurity awareness among urban schoolteachers: A study on preparedness and digital safety practices. Journal of Cyber Education, 8(3), 221-236.